

**Medical Care Collection Fund (MCCF)  
Electronic Data Interchange (EDI)  
Transaction Applications Suite (TAS)  
ePharmacy Build 20**

**Electronic Claims Management Engine BPS\*1.0\*32  
Outpatient Pharmacy PSO\*7.0\*648  
CMOP PSX\*2.0\*93**

**Deployment, Installation, Back-out, and Rollback  
Guide**



**August 2022**

**Department of Veterans Affairs**

**Office of Information and Technology (OIT)**

## Revision History

Date	Version	Description	Author
August 2022	1.0	Initial Version	EDI TAS ePharmacy Development Team

## Artifact Rationale

This document describes the Deployment, Installation, Back-out, and Rollback Plan for new products going into the VA Enterprise. The plan includes information about system support, issue tracking, escalation processes, and roles and responsibilities involved in all those activities. Its purpose is to provide clients, stakeholders, and support personnel with a smooth transition to the new product or software, and should be structured appropriately, to reflect particulars of these procedures at a single or at multiple locations.

Per the Veteran-focused Integrated Process (VIP) Guide, the Deployment, Installation, Back-out, and Rollback Plan is required to be completed prior to Critical Decision Point #2 (CD #2), with the expectation that it will be updated throughout the lifecycle of the project for each build, as needed.

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Purpose .....	1
1.2	Dependencies .....	1
1.3	Constraints.....	1
<b>2</b>	<b>Roles and Responsibilities.....</b>	<b>1</b>
<b>3</b>	<b>Deployment .....</b>	<b>2</b>
3.1	Timeline.....	2
3.2	Site Readiness Assessment .....	2
3.2.1	Deployment Topology (Targeted Architecture).....	2
3.2.2	Site Information (Locations, Deployment Recipients).....	3
3.2.3	Site Preparation .....	3
3.3	Resources .....	3
3.3.1	Facility Specifics .....	3
3.3.2	Hardware .....	3
3.3.3	Software .....	3
3.3.4	Communications .....	4
3.3.4.1	Deployment / Installation / Back-out Checklist.....	4
<b>4</b>	<b>Installation .....</b>	<b>4</b>
4.1	Pre-installation and System Requirements .....	4
4.2	Platform Installation and Preparation .....	5
4.3	Download and Extract Files .....	5
4.4	Database Creation .....	5
4.5	Installation Scripts.....	5
4.6	Cron Scripts .....	5
4.7	Access Requirements and Skills Needed for the Installation .....	5
4.8	Installation Procedure .....	5
4.9	Installation Verification Procedure.....	6
4.10	System Configuration .....	6
4.11	Database Tuning.....	6
<b>5</b>	<b>Back-out Procedure .....</b>	<b>6</b>
5.1	Back-out Strategy .....	6
5.1.1	Mirror Testing or Site Production Testing.....	6
5.1.2	After National Release but During the Designated Support Period .....	6
5.1.3	After National Release and Warranty Period.....	6
5.2	Back-out Considerations .....	7
5.2.1	Load Testing.....	7
5.2.2	User Acceptance Testing.....	7
5.3	Back-out Criteria.....	8
5.4	Back-out Risks.....	9

5.5	Authority for Back-out.....	9
5.6	Back-out Procedure.....	9
5.7	Back-out Verification Procedure .....	9
6	Rollback Procedure.....	10
6.1	Rollback Considerations.....	10
6.2	Rollback Criteria .....	10
6.3	Rollback Risks .....	10
6.4	Authority for Rollback .....	10
6.5	Rollback Procedure .....	10
6.6	Rollback Verification Procedure.....	10

## List of Tables

Table 1:	Deployment, Installation, Back-out, and Rollback Roles and Responsibilities .....	1
Table 2:	Site Preparation .....	3
Table 3:	Facility-Specific Features .....	3
Table 4:	Hardware Specifications .....	3
Table 5:	Software Specifications.....	4
Table 6:	Self Identified Gender Field.....	8
Table 7:	Sex Field Value .....	8

# 1 Introduction

This document describes how to deploy and install the multi-build BPS PSO PSX BUNDLE 20.0 (includes BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93) and how to back-out the product and rollback to a previous version or data set.

## 1.1 Purpose

The purpose of this plan is to provide a single, common document that describes how, when, where, and to whom the multi-build BPS PSO PSX BUNDLE 20.0 (includes BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93) will be deployed and installed, as well as how it is to be backed out and rolled back, if necessary. The plan identifies resources, communications plan, and rollout schedule. Specific instructions for installation, back-out, and rollback are included in this document.

## 1.2 Dependencies

BPS\*1\*27 and BPS\*1\*30 must be installed BEFORE BPS\*1\*32.

PSO\*7\*562 must be installed BEFORE PSO\*7\*648.

PSX\*2\*92 must be installed BEFORE PSX\*2\*93.

## 1.3 Constraints

This patch is intended for a fully patched VistA system.

# 2 Roles and Responsibilities

**Table 1: Deployment, Installation, Back-out, and Rollback Roles and Responsibilities**

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
1	VA OIT, VA OIT Health Product Support, and PMO (Leidos)	Deployment	Plan and schedule deployment (including orchestration with vendors)	Planning
2	Local VAMC and CPAC processes	Deployment	Determine and document the roles and responsibilities of those involved in the deployment.	Planning
3	Field Testing (Initial Operating Capability - IOC), Health Product Support Testing & VIP Release Agent Approval	Deployment	Test for operational readiness	Testing

ID	Team	Phase / Role	Tasks	Project Phase (See Schedule)
4	Health Product Support and Field Operations	Deployment	Execute deployment	Deployment
5	Individual Veterans Administration Medical Centers (VAMCs)	Installation	Plan and schedule installation	Deployment
6	VIP Release Agent	Installation	Ensure authority to operate and that certificate authority security documentation is in place	Deployment
7		Installation	Validate through facility POC to ensure that IT equipment has been accepted using asset inventory processes	N/A; only existing VistA system will be used
8	VA's eBusiness team	Installations	Coordinate training	Deployment
9	VIP Release Agent, Health Product Support & the development team	Back-out	Confirm availability of back-out instructions and back-out strategy (what are the criteria that trigger a back-out)	Deployment
10	VA OIT, VA OIT Health Product Support, and MCCF EDI TAS Development Team (Halfaker)	Post Deployment	Hardware, Software and System Support	Warranty

### 3 Deployment

The deployment is planned as a national rollout.

This section provides the schedule and milestones for the deployment.

#### 3.1 Timeline

The deployment and installation are scheduled to run for 30 days starting with national release.

#### 3.2 Site Readiness Assessment

This section discusses the locations that will receive the deployment of the multi-build BPS PSO PSX BUNDLE 20.0 (includes BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93).

##### 3.2.1 Deployment Topology (Targeted Architecture)

This multi-build BPS PSO PSX BUNDLE 20.0 (includes BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93) is to be nationally released to all VAMCs.

## 3.2.2 Site Information (Locations, Deployment Recipients)

The IOC sites are:

- Birmingham
- Eastern Kansas
- Lexington
- Richmond

## 3.2.3 Site Preparation

The following table describes preparation required by the site prior to deployment.

**Table 2: Site Preparation**

Site / Other	Problem / Change Needed	Features to Adapt / Modify to New Product	Actions / Steps	Owner
N/A	N/A	N/A	N/A	N/A

## 3.3 Resources

### 3.3.1 Facility Specifics

The following table lists facility-specific features required for deployment.

**Table 3: Facility-Specific Features**

Site	Space / Room	Features Needed	Other
N/A	N/A	N/A	N/A

### 3.3.2 Hardware

The following table describes hardware specifications required at each site prior to deployment.

**Table 4: Hardware Specifications**

Required Hardware	Model	Version	Configuration	Manufacturer	Other
Existing VistA system	N/A	N/A	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 for details about who is responsible for preparing the site to meet these hardware specifications.

### 3.3.3 Software

The following table describes software specifications required at each site prior to deployment.

**Table 5: Software Specifications**

<b>Required Software</b>	<b>Make</b>	<b>Version</b>	<b>Configuration</b>	<b>Manufacturer</b>	<b>Other</b>
Fully patched Electronic Claims Management Engine package within VistA	N/A	1.0	N/A	N/A	N/A
Fully patched Outpatient Pharmacy package within VistA	N/A	7.0	N/A	N/A	N/A
Fully patched CMOP package within VistA	N/A	2.0	N/A	N/A	N/A

Please see the Roles and Responsibilities table in Section 2 above for details about who is responsible for preparing the site to meet these software specifications.

### **3.3.4 Communications**

The sites that are participating in field testing (IOC) will use the “Patch Tracking” message in Outlook to communicate with the ePharmacy eBusiness team, the developers, and product support personnel.

#### **3.3.4.1 Deployment / Installation / Back-out Checklist**

The Release Management team will deploy the multi-build BPS PSO PSX BUNDLE 20.0, which is tracked nationally for all VAMCs in the National Patch Module (NPM) in Forum. Forum automatically tracks the patches as they are installed in the different VAMC production systems. One can run a report in Forum to identify when and by whom the patch was installed into the VistA production at each site. A report can also be run to identify which sites have not currently installed the patch into their VistA production system. Therefore, this information does not need to be manually tracked in the chart below.

**Table 6: Deployment / Installation / Back-out Checklist**

<b>Activity</b>	<b>Day</b>	<b>Time</b>	<b>Individual who completed task</b>
Deploy	N/A	N/A	N/A
Install	N/A	N/A	N/A
Back-out	N/A	N/A	N/A

## **4 Installation**

### **4.1 Pre-installation and System Requirements**

Multi-build BPS PSO PSX BUNDLE 20.0 is installable on a fully patched M(UMPS) VistA system and operates on the top of the VistA environment provided by the VistA infrastructure packages. The latter provides utilities that communicate with the underlying operating system



and hardware, thereby providing each VistA package independence from variations in hardware and operating system.

## **4.2 Platform Installation and Preparation**

Refer to the BPS\*1.0\*32 documentation on the NPM in Forum for the detailed installation instructions. These instructions include any pre-installation steps if applicable.

## **4.3 Download and Extract Files**

Refer to the BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93 documentation on the NPM to find related documentation that can be downloaded. The patch description of each patch will be transmitted as a MailMan message from the NPM. These messages can also be pulled from the NPM. The patches themselves are bundled together into the multi-build BPS PSO PSX BUNDLE 20.0. The host file containing these patches must be downloaded separately. The file name is BPS\_1\_32\_PSO\_PSX.KID and it can be found on the [VistA software download site](#).

## **4.4 Database Creation**

Multi-build BPS PSO PSX BUNDLE 20.0 modifies the VistA database. All changes can be found on the NPM documentation for this patch.

## **4.5 Installation Scripts**

No installation scripts are needed for multi-build BPS PSO PSX BUNDLE 20.0 installation.

## **4.6 Cron Scripts**

No Cron scripts are needed for multi-build BPS PSO PSX BUNDLE 20.0 installation.

## **4.7 Access Requirements and Skills Needed for the Installation**

Staff performing the installation of this multi-build will need access to FORUM's NPM to view all patch descriptions. Staff will also need access and ability to download the host file from the VistA software download site. The software is to be installed by each site's or region's designated VA OIT IT Operations Service, Enterprise Service Lines, VistA Applications Division<sup>1</sup>.

## **4.8 Installation Procedure**

Detailed instructions for installing the multi-build BPS PSO PSX BUNDLE 20.0 (includes BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93) can be found on the patch description for BPS\*1.0\*32, which can be found on the NPM. Installing the multi-build BPS PSO PSX

---

<sup>1</sup> "Enterprise service lines, VAD" for short. Formerly known as the Information Resources Management (IRM) or IT support.

BUNDLE 20.0 will install all component patches (BPS\*1.0\*32, PSO\*7.0\*648, and PSX\*2.0\*93).

## **4.9 Installation Verification Procedure**

Refer to the BPS\*1.0\*32 documentation on the NPM for detailed installation instructions. These instructions include any post installation steps if applicable.

## **4.10 System Configuration**

No system configuration changes are required for this patch.

## **4.11 Database Tuning**

No reconfiguration of the VistA database, memory allocations, or other resources is necessary.

# **5 Back-out Procedure**

Back-out pertains to a return to the last known good operational state of the software and appropriate platform settings.

## **5.1 Back-out Strategy**

A decision to back out could be made during Site Mirror Testing, during Site Production Testing, or after National Release to the field (VAMCs). The best strategy decision is dependent on the stage during which the decision is made.

### **5.1.1 Mirror Testing or Site Production Testing**

If a decision to back out is made during Mirror Testing or Site Production Testing, a new version of the patch can be used to restore the build components to their pre-patch condition.

### **5.1.2 After National Release but During the Designated Support Period**

If a decision to back out is made after national release and within the designated support period, a new patch will be entered into the NPM in Forum and will go through all the necessary milestone reviews, etc. as a patch for a patch. This patch could be defined as an emergency patch, and it could be used to address specific issues pertaining to the original patch or it could be used to restore the build components to their original pre-patch condition.

### **5.1.3 After National Release and Warranty Period**

After the 90-day warranty period, the VistA Maintenance Program will produce the new patch, either to correct the defective components or restore the build components to their original pre-patch condition.

## 5.2 Back-out Considerations

Changes implemented with multi-build BPS PSO PSX BUNDLE 20.0 can be backed out in their entirety or on an enhancement-by-enhancement basis. Either could be accomplished via a new version of multi-build BPS PSO PSX BUNDLE 20.0 if before national release or a new multi-build if after national release.

### 5.2.1 Load Testing

N/A. The back-out process will be executed at normal rather than raised job priority and is expected to have no significant effect on total system performance. After the reversion, the performance demands on the system will be unchanged.

### 5.2.2 User Acceptance Testing

Below are the acceptance criteria for each story included in BPS PSO PSX BUNDLE 20.0.

#### EPHAR-1614

- The REJ action works correctly for pseudo rejects (eT,eC) for refills.
- The REJ continues to work on the pseudo reject for the original fills as expected. Regression.
- The REJ continues to work on all other rejects (those other than eT,eC) as expected. Regression.
- Rejects access from the Worklist continue to work as expected. Regression.

#### EPHAR-2146

- If the VistA Self Identified Gender field (Patient file #2, field # .024) is populated, the appropriate ECL value will transmit in the NCPDP field 305-C5 Patient Gender Code.
- If the VistA Self Identified Gender field (Patient file #2, field # .024) is not populated, then ePharmacy will use the value in the VistA Sex field (Patient file #2, field # .02) and the appropriate ECL value will transmit in the NCPDP field 305-C5 Patient Gender Code.

#### EPHAR-2646

- The RED Resubmit w/Edits action contains a new field “Patient Gender Code” that appears after “Delay Reason Code:”
- Patient Gender Code in RED will default to Self-Identified Gender field, if populated, from the Patient file.  
If Self-Identified is not populated, the system will use the Birth Sex field from the Patient File.
- Entering ? will display the message:  
Available Gender Codes are determined by the VistA Patient File.

Choose from:

- M Male (Birth Sex)
- TF Transgender Female (Self-Identified Gender)

Selection will display the abbreviation and the description of the valid entries for the patient.

- The User can enter the abbreviation or partial / full description of the available gender codes.
- The system will populate the Patient Gender Code NCPDP field based on the user response and the crosswalk.

**Table 6: Self Identified Gender Field**

Self Identified Gender Field Value	ePharmacy Numeric Value / Definition
Male	1 – Male
Female	2 – Female
Non-Binary	3 – Non-Binary
Doesn't disclose	0 – Not specified
Other	3 – Non-Binary
Transgender Male	3 – Non-Binary
Transgender Female	3 – Non-Binary

**Table 7: Sex Field Value**

Sex Field Value	ePharmacy Numeric Value / Definition
Male	1 – Male
Female	2 – Female

- If an incorrect entry is made, the system will provide the acceptable responses.
- System will echo the valid selection.
- If the Self-Identified Gender field is not populated, the only available response displayed to the user in RED will be the Birth Sex.

## 5.3 Back-out Criteria

It may be decided to back out this patch if the project is canceled, the requested changes implemented by multi-build BPS PSO PSX BUNDLE 20.0 are no longer desired by VA OIT and the ePharmacy eBusiness team, or the patch produces catastrophic problems.

## 5.4 Back-out Risks

Since the ePharmacy software is tightly integrated with external systems, any attempt at a back-out should include close consultation with the external trading partners such as the Financial Services Center (FSC) and the Health Care Clearing House (HCCH) to determine risk.

## 5.5 Authority for Back-out

Any back-out decision should be a joint decision of the Business Owner (or their representative) and the Program Manager with input from the Health Services Portfolio (HSP) Application Coordinator, developers (both project and Tier 3 HSP), and if appropriate, external trading partners such as the VA FSC or Change Healthcare.

## 5.6 Back-out Procedure

The back-out plan for VistA applications is complex and not a “one size fits all” solution. The general strategy for a VistA back-out is to repair the code with a follow-up patch. The development team recommends that sites log a ticket if it is a nationally released patch.

If it is prior to national release, the site will be already working directly with the development team daily and should contact that team. The development team members will have been identified in the Initial Operating Capability (IOC) Memorandum of Understanding (MOU). As discussed in section 5.2, it is likely that development team can quickly address via a new software version. If the site is unsure whom to contact, they may log a ticket or contact Health Services Portfolio - Management Systems Team.

Multi-build BPS PSO PSX BUNDLE 20.0 contains the following build components:

- Routines
- Data Dictionaries
- Files

While the VistA KIDS installation procedure allows the installer to back up the modified routines using the ‘Backup a Transport Global’ action, the back-out procedure for global, data dictionary, and other VistA components is more complex and requires issuance of a follow-up patch to ensure all components are properly removed and/or restored. All software components (routines and other items) must be restored to their previous state at the same time and in conjunction with the restoration of the data.

Please contact the EPMO team for assistance since this installed patch contains components in addition to routines.

## 5.7 Back-out Verification Procedure

Successful back-out is confirmed by verification that the back-out patch was successfully implemented. This includes successful installation and testing that the back-out acts as expected, as defined together with the team the site contacted in section 5.5.

## **6 Rollback Procedure**

Rollback pertains to data. The data changes in this patch are specific to the operational software and platform settings. These data changes are covered in the Back-out procedures detailed elsewhere in this document.

### **6.1 Rollback Considerations**

Not applicable.

### **6.2 Rollback Criteria**

Not applicable.

### **6.3 Rollback Risks**

Not applicable.

### **6.4 Authority for Rollback**

Not applicable.

### **6.5 Rollback Procedure**

Not applicable.

### **6.6 Rollback Verification Procedure**

Not applicable.